iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VIII **Month of publication:** August 2020

DOI: https://doi.org/10.22214/ijraset.2020.30837

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VIII Aug 2020- Available at www.ijraset.com

Blockchain Technology and its Applications - An Overview

J. Uma Maheswari[1], S. Vijayalakshmi[2], G. R. Karpagam[3]
[1, 2, 3]*Department of Computer Science and Engineering, PSG College of Technology*

Abstract: ***Blockchain technology is the key for decentralized society and gathered a lot of attention in recent times. The technology of Blockchain offers an infrastructure of secure network that allows the users to perform any operation without middleman. It is expected to bring a revolution due to its characteristics of being transparent, secure and scalable. Blockchain technology will bring the considerable efficiency gains, transparency, cost savings and fraud detection while allowing the data to be shared in real-time between multiple parties in a trusted and transparent manner. This chapter elaborately discusses the basic building blocks of Blockchain technology such as public key cryptography, Digital signature, Elements and types of Blockchain and its applications in different sectors.***

Keywords: ***Blockchain, Bitcoin, Elliptic curve Digital signature Algorithm, Double spending, Attacks***

I. INTRODUCTION

Blockchain is a chain of blocks in which the information of transactions is recorded and maintained in a distributed public ledger across a number of computers that are linked in a peer-to-peer network. Blockchain was first introduced by [1] who proposed a peer -to-peer payment system that allows cash transactions through the Internet without relying on the need for a financial institution. Blockchain is secure by design, and an example of a system with a high byzantine failure tolerance [2]. Bitcoin is the first application of the Blockchain concept to create a currency that could be exchanged over the internet using cryptography to secure the transactions. Bitcoin blockchain is the mother of all blockchain. Blockchain is an ordered data structure that contains blocks of transactions. Each block in the blockchain is linked to the previous block in the chain. The first block in the chain is referred to as the Genesis block. Each block created gets layered on top of the previous block to form a stack called a Blockchain. There are a set of rules for confirmation of the legitimacy of a block and to verify that block has not been altered maliciously. Blockchain technology solved the problem of *Double-spending* (the event where customer can spend a set of the same bitcoins in two different transactions) as the second transaction would be recognized as invalid.

II. BUILDING BLOCKS OF BLOCKCHAIN

A. Public key cryptography

In Public key cryptography two keys are used, one is called the private key and the other is called the public key. Public key cryptography is a fundamental part of Blockchain and is utilized to guarantee the integrity of the messages and transactions incorporated with the blocks. The Blockchain utilizes the Elliptic Curve Digital Signature Algorithm (ECDSA) shown in Fig 1 to make an arrangement of private keys and a related public key. The public key is used with the hash(SHA-256) function to create a general address which is used by the public to carry out the transactions. The private key is kept secret and is utilized to sign a digital exchange to ensure exchange is genuine.

B. Digital Signature

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital document. A legitimate digital signature gives a recipient reason to trust that the message was created and sent by a known sender. It is significant to detect forgery or tampering. Along with authentication, it also possess the property of integrity, which ensures that the received digital documents are not modified / manipulated or altered during the transmission of digital documents from sender to receiver. Digital signature is a key feature for Blockchain transaction. Every transaction has a different digital signature which relies on the private key of the sender. Additionally, given the message, the public key of the sender and the digital signature, it is non-trivial to check if the signature is legitimate. The sender signs the exchange, sent to the miners. The miner make use of the sender's public key to guarantee that the digital signature is authentic which renders a hacker incapable of spending senders' assets without their consent. Once the digital signature is verified, the transaction is added to the new block and the money is exchanged from one wallet (account) to another.

Key Generation

The ECDSA key-pair (pricey, pubKey) consists of

- *priKey:* private key is a random integer in the range [0...*n*-1]
- *pubKey* = *priKey* * G (the private key, multiplied by the generator point G)

Signature Generation

1. Calculate the message hash h, using a cryptographic hash function *h* = hash(*message*)
2. Generate a random number *k* in the range [1..*n*-1]
3. Calculate the random point *R* = *k* * G and take its x-coordinate: *r* = *R*.x
4. Calculate the signature $s = k^{-1} * (h + r * priKey) (mod\ n)$
5. Return the signature {*r*, *s*}.

The calculated signature {*r*, *s*} is a pair of integers, each in the range [1...*n*-1].

Signature Verification

To verify a signature takes as input the signed message *msg*, the signature {*r*, *s*} and the public key *pubKey*, corresponding to the signer's private key. The output is boolean value: *valid* or *invalid* signature. The ECDSA signature verification algorithm works as follows.

1. Calculate the message hash, using the same cryptographic hash function used during the signing process: *h* = hash(*msg*)
2. Calculate the modular inverse of the signature: *s1* $= S^{-1} (mod\ n)$
3. Recover the random point used during the signing: *R'* = (*h* * s1) * G + (*r* * *s1*) * *pubKey*
4. Obtain from *R'* its x-coordinate: *r'* = *R'*.x
5. Calculate the signature validation result by comparing whether *r'* == *r*

The common idea of the signature verification is to recover the point *R'* using the public key and check whether it is same point *R*, generated randomly during the signing process.

Fig 1 Elliptic Curve Digital Signature Algorithm (ECDSA)

III.BLOCKCHAIN TECHNOLOGY

Blockchain is about enabling peer to peer transaction in a decentralized network, establishing trust among unknown peers (by having a process in place to validate, verify, and confirm transactions), recording the transaction in an immutable distributed ledger of blocks (create a tamper-proof record of blocks, chain of blocks, and implement a consensus protocol for agreement on the block to be added to the chain). The Bitcoin stores the transaction information as a set, encompassing the sender information, the receiver information and the amount transferred. Each Block has a unique block id (hash value), which can be compared to a fingerprint. When a block is created, its hash value is calculated concurrently, and any changes of the information in that block will change the corresponding hash value.

A. Generic Elements of a Blockchain

The core Blockchain architecture is shown in Figure 2. The components or elements are expressed as follows:

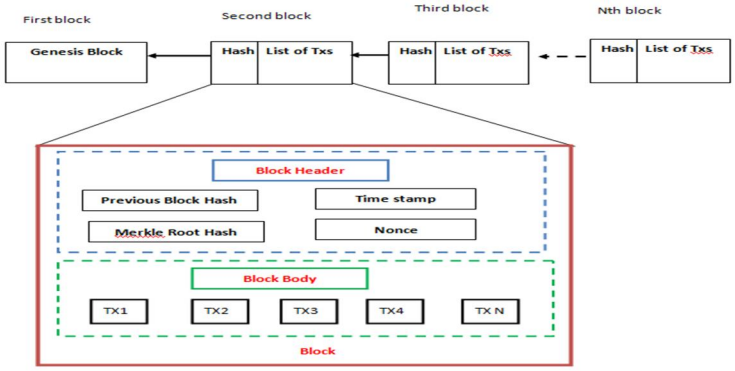


Figure 2.Blockchain architecture

1) *Genesis Block:* is the first block in the Blockchain that was hardcoded at the time of the commencement of the Blockchain. It is the foundation on which further blocks are sequentially added to form a chain of blocks as it contains only one transaction.
2) *Block:* is a data structure used for keeping a collection of transactions that is distributed to all nodes in the peer to peer network.
3) *Nonce:* is a number that is generated and used only once. It is used in Proof of Work (PoW) consensus algorithms for transaction reply protection.
4) *Merkle Root:* In each block, the transactions are stored using Merkle Tree. It is used to verify the contents of the block and consistency of multiple ledgers. If one copy of the Blockchain has the same Merkle root for a block as another copy of the Blockchain, then all the transactions in that block are the same and agree on the ledger. Even a tiny variation would lead to very much different Merkle roots because of the properties of a hash.
5) *Node:* user/computer within the Blockchain architecture. A node can propose, validate a transaction and perform mining tasks to facilitate consensus and secure the Blockchain. Each node has an independent copy of the whole Blockchain ledger.
6) *Miners:* specific nodes which perform the block verification process before adding to the Blockchain structure
7) *Consensus Mechanisms:* that replaces the need for a trusted third party. It ensures the number of nodes (threshold) which must agree on the validity of new blocks before they can become part of the network. Miners" use various mining to control and certify the transactions, ranging from proof-of-work and proof-of-stake, etc
8) Proof-of-work (PoW) probabilistically calculates the work of a node with an energy-intensive cryptographic puzzle and sends the reward to the first node. The computational power needed to resolve the cryptographic puzzle is proportional to the probability of being the first to solve it [3]. A major weakness of proof-of-work systems remains in the inefficiency of having many miners competing to mine blocks by engaging in energy-intensive tasks but only the winner effectively mines a block.
9) Proof-of-stake (PoS) mining protocol allocates mining work according to the miner's wealth, rather than their computing power (Hjalmarsson et.al. 2018). The nodes holding the assets of the network thus have the strongest incentive to maintain the security and viability of the network. Advantages of proof-of-stake, compared to proof-of-work, include reduced energy waste, lower likelihood of computation power.
10) *Smart contract:* is a piece of code deployed in the blockchain node. These are automated, autonomous programs that reside on the Blockchain network and encapsulate the business logic and code needed to execute a specific function when certain conditions are met.

B. Types of Blockchain

There are three types of Blockchain in use. These are:

1) Public Blockchain: the data and access to the blockchain is available to anyone who is willing to participate.
2) Private Blockchain: opposed to the public Blockchain, the private blockchain is controlled only by a selected organization or authorized users who have permission for participation.
3) Consortium Blockchain: consist of a few organizations or consortium. In a consortium, procedures are set up and controlled by the previously assigned users.

C. How Miners work in Blockchain Technology

This section describes how to include a block in bitcoin Blockchain. Blockchain uses the concept called link-list which store transaction history of the whole system in blocks. In each block except the genesis block, the transactions are stored using Merkle Tree. A secure time-stamp, nonce and a hash of the previous block is also stored [4].

The procedure for crating and adding a new block to the network is as follows:

1) Transactions are initiated and validated
2) Transactions are bundled and broadcasted to all peers in the blockchain
3) The miners need to mine a block by performing a computationally difficult Proof of Work (PoW) puzzle.
4) Once a miner solved the PoW puzzle for a block, it adds the block in his local Blockchain and broadcasts the solution throughout the network and after getting a solution for valid block, miners quickly check the solution and add the block to their Blockchain.

Due to distributed nature of the block validation process, it is possible that two valid puzzle solutions may be determined at the same time. This causes a delay in the distribution of a valid block. If there are two valid solutions exits then this is called a 'Fork' in Blockchain. When numerous forks exist, the miners can select a fork and proceed to mine over it. If the system has several forks and miners are extending different but valid versions of Blockchain based on their local Blockchain, miners working on one fork may

communicate a valid block before miners working on another fork [5]. This result in a more extended version of the Blockchain in the system, and any miner can add new blocks on top of this longer Blockchain.

D. The Application of Blockchain

There are many areas in which Blockchain [6] can be used as a secured decentralized storage. The following section describes some of the applications of Blockchain.

1) *Health Care:* In the existing electronic medical health record management systems the medical data are controlled by the clinicians. Instead the medical records of patients are stored in the blockchain. Also it allows patients to decide on distributing their medical records. When a doctor needs the patient's medical record then patient or family member must explicitly permit the doctor for accessing the patient's medical record. Furthermore, every time an access to a particular patient's data is made, this event is captured in the Blockchain's immutable transaction history, which allows the patient to find if anyone has accessed or modified the data.
2) *Blockchain Enabled IOT:* The IoT consists of several components that sense and gather data from their environment, which is used to perform automated functions to help humans. The introduction of wearable devices, the falling prices of components increases the popularity of IoT in the areas such as home, precision agriculture, infrastructure monitoring, personal healthcare and autonomous vehicles etc. Data collected by IoT devices may contain important information which can be stored in Blockchain [10] for raising severe privacy and security concerns.
3) *Inventory:* This system also aims to use blockchain technology for storing the details of drugs and equipment purchases carried out by the hospital for the following reasons. First, blockchain makes it possible to have an immutable record of the drugs and equipment thereby avoiding the denial of purchase by the hospital authorities or denial of supply by the suppliers [8]. Second, it allows reliable tracking of transactions between hospital and supplier, leading to a greater cost-efficacy and accountability of hospital systems. This type of process can be used in all types of inventory system in various industries like chemical, mechanical and production industries.
4) *Service Level Agreements:* All services may not be available with the users or business companies. They are in need of some service providers in order to get and use the services. There are huge benefits to the user as they can spend less time and less cost on energy, management and construction. So, this makes them to move on to the usage of external services. Small companies make use of the external services for converting their ideas into products rather than spending lot of time in implementing the required services. Thus, their product deployment is as fast as possible and hits the market amidst other competitive products. Some agreements will be signed by both the party members i.e. the users of the services and the service providers. It contains many qualities of service parameters such as availability, performance, scalability and many other things. The service providers will assure some percentage value to QOS parameters which the users experiences. But in reality the user may not experience the quality of service as mentioned in the service level agreement. So, by using the concept of block chaining, it is desirable to find the difference between the users experienced value of the QOS parameters and the value given by the service provider. If the difference is higher than the service consumer can get the penalty from the service provider.
5) *Asset Management:* The management of assets like land or house requires significant processing of sensitive and costly trading related transactions among several parties. Everybody wish to keep their own copy of the document. Instead of having multiple copies of same records of transactions by wasting space and resources Blockchain can be used to store those records it reduces human errors.
6) *Insurance:* Blockchain technology will bring the considerable efficiency gains, transparency, cost savings and fraud detection while allowing the data to be shared in real-time between multiple parties in a trusted and transparent manner. Insurance companies run in a highly competitive environment and they need recent as well as trustable data for processing insurance. Customer, Hospital, Government and Insurance Company related records are stored in a Blockchain then no one can give the false information. So Blockchain[7] can be used as a trustable platform when multiple parties are involved in the transaction.
7) *Voting:* Online voting gives guarantees to improve the democratic participation as it allows casting the votes from remote locations. It is one of the cost effective solution that speeds up the tallying process and helps in increasing voter turnout. The security [11] aspect of online voting is a vital significance. A Blockchain is a peer to peer, distributed ledger that is cryptographically secure, append only, immutable and updateable via consensus. All the characteristics of Blockchain match the exact requirements of online voting. It is desirable to use Blockchain for online voting to satisfy higher security constraints.
8) *Loan Management:* Blockchain-based smart contracts ensure that both loan borrowers and lenders agree to neutral and feasible terms regarding things like payment and re payment planning. This contract provides a way for direct communication between

sender and the receiver without middlemen which leads to increase the cost of processing. All the transactions of lender and borrower can be recorder in the ledger for security purpose. Blockchain [9] based loan processing platforms speed up loan processing times and reduces the cost.

9) *Media:* The Internet became faster and widely used, users were able to download any song they wanted without paying .The free downloading of music and using it anywhere had serious consequence for the musicians which include financial loss. The same situation happened for movies also. Because of good Internet speeds and huge computer storage made downloading movies in short time and some movies are released in internet itself claiming intellectual property rights for the corresponding owner is difficult task. Blockchain is a way to solve the problem of illegal usage of music, frames and movies.

E. Attacks on Blockchain

1) Due to the decentralized nature of its working environment, attackers have launched numerous attacks over the blockchain technology. The primary attack vectors include

2) Selfish Mining Attack is one of the Consensus Mechanism and Mining-based Attacks. In reality, every one of the miners in Bitcoin is mining for the reward that is related with each block. However these miners are also valid and reasonable node. In the selfish mining, the dishonest miners perform data hiding and damage other honest or valid miners by obtaining an unfair compensation which is greater than their offer of processing control spent. This attack affects all applications because blocks are added to Blockchain by miners. When miners are adding invalid blocks it becomes difficult to add valid blocks This type of attack occurs in applications such as Government Services, IoT , Smart Contracts, Identity and Financials etc.

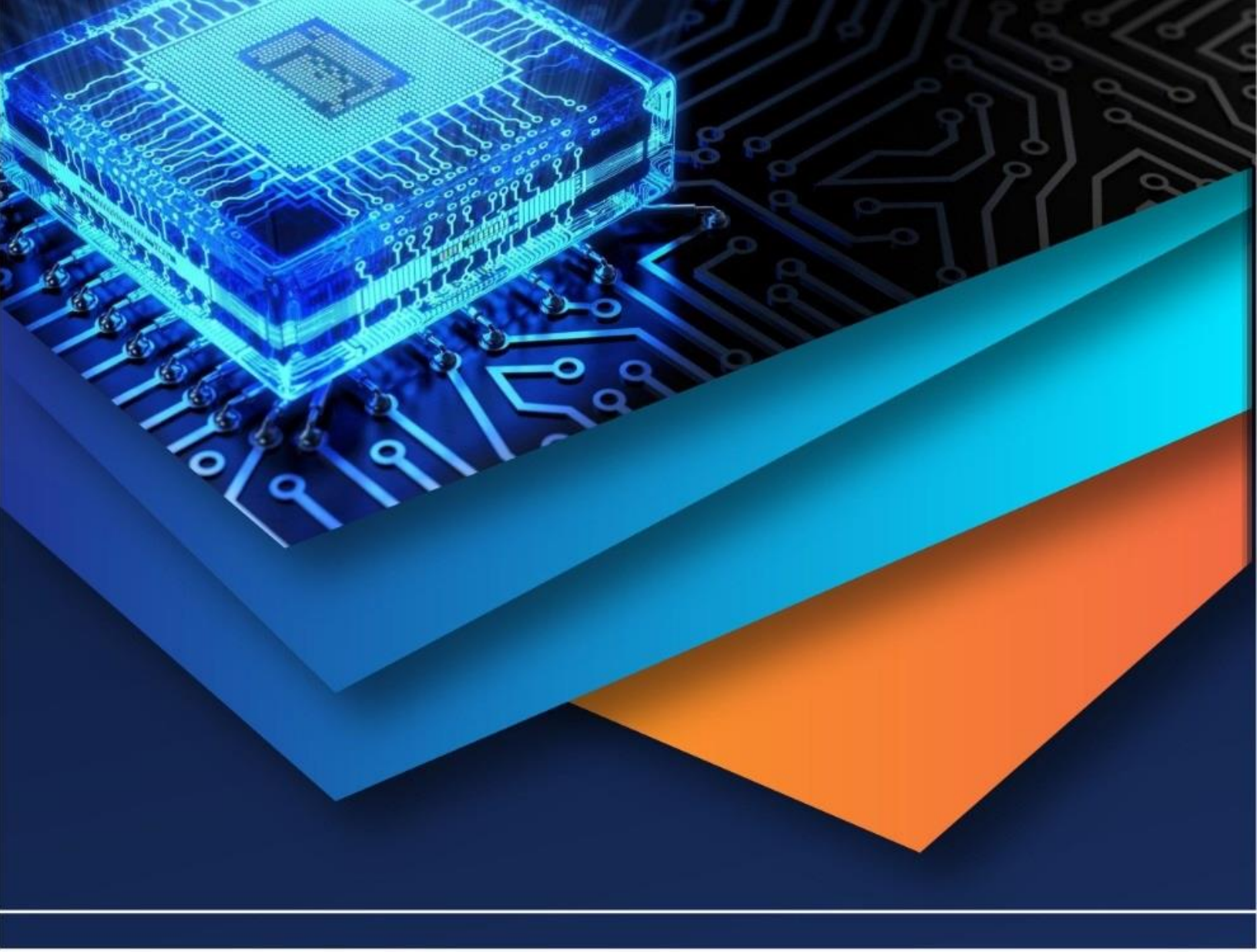
3) Sybil Attack is a type of Peer-to-Peer Network-based Attacks where the attacker installs dummy software and tries to compromise part of the Blockchain network. A Sybil attack is also called as a community-based attack performed by a group of comprised nodes. The main objective is not to target one, but a network as whole, and generate a fork in the blockchain if possible. There is a possibility of this type of attack presents in the applications such as smart contracts, government services, financial services etc.

IV. CONCLUSION

In this paper, we provided a widespread survey of certain basics which brings the Blockchain technology to maturity and addressed the core features of the Blockchain technology, which is a distributed ledger with immutable and verifiable transaction records. Specific focus were given to different areas in which current research efforts have been increased in designing and developing blockchain-based platforms, applications, and services.

REFERENCES

[1] S.Nakamoto, Bitcoin: A peer-to-peer electronic cash system. Available from: https://www.dhimmel/bitcoin-whitepaper@a5f36b3,2018.
[2] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System", *Security and Privacy in Social Networks*, 2013, pp. 1-27.
[3] Silhavy, R, Silhavy, P & Prokopová, Z, 'Architecture of COOPTO remote voting solution,' *Advanced Techniques in Computing Sciences and Software Engineering* , 2010, pp. 477- 479.
[4] D. Kraft, "Difficulty control for blockchain-based consensus systems, *Peer-to-Peer Networking and Applications*, 2016,vol. 9, no. 2, pp. 397–413.
[5] Szabo, N, Secure Property Titles with Owner Authority. Satoshi Nakamoto Institute. [online] Nakamotoinstitute.org. Available at: nakamotoinstitute.org/secure-property-titles/, 2018
[6] Rahul Rao Vokerla, Bharanidharan Shanmugam , Sami Azam, Asif Karim, Friso De Boer, Mirjam Jonkman, Fahad Faisal, An Overview of Blockchain Applications and Attacks, *International Conference on Vision Towards Emerging Trends in Communication and Networking*, 2019.
[7] Zhao, J., Fan, S. and Yan, J, Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financial *Innovation*, 2016, 2(1).
[8] Provenance, Blockchain: the solution for transparency in product supply chains. Whitepaper, 2015.
[9] Blockgeeks, smart Contracts: The Blockchain Technology That Will Replace Lawyers. [online] Available at: https://blockgeeks.com/guides/smart-contracts/,2019
[10] Marr, B., 35 Amazing Real World Examples Of How Blockchain Is Changing Our World. [online] Available at: https://www.forbes.com/sites/bernardmarr/2018/01/22/35-amazing-real- world-examples-of-how-blockchain-is-changing-our-world, 2018.
[11] S VIJAYALAKSHMI, G R KARPAGAM, SECURE ONLINE VOTING SYSTEM IN CLOUD, *ELECTRONIC GOVERNMENT, AN INTERNATIONAL JOURNAL*, 2018,14 (3), 276-286



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY